

# RELATIVE GENERALIZED HAMMING WEIGHTS OF CYCLIC CODES

JUN ZHANG AND KEQIN FENG

**ABSTRACT.** Relative generalized Hamming weights (RGHWs) of a linear code respect to a linear subcode determine the security of the linear ramp secret sharing scheme based on the code. They can be used to express the information leakage of the secret when some keepers of shares are corrupted. Cyclic codes are an interesting type of linear codes and have wide applications in communication and storage systems. In this paper, we investigate the RGHWs of cyclic codes with two nonzeros respect to any of its irreducible cyclic subcodes. Applying the method in [1], we give two formulae for RGHWs of the cyclic codes. As applications of the formulae, explicit examples are computed.

## 1. INTRODUCTION

A secret sharing scheme splits a secret into several pieces which are distributed to participants, so that only specified subsets of participants can recover the secret. Shamir [2] proposed the first secret sharing scheme in which the subsets of participants unable to reconstruct the secret can not get any information about the secret. A secret sharing scheme with this property is called a perfect scheme. Later, realizing that Shamir's construction is indeed from Reed-Solomon codes [3], Shamir's construction was generalized to secret sharing schemes based on linear codes [4, 5, 6]. All these constructions are perfect schemes. The security of secret sharing schemes based on linear codes are completely characterized by the minimal codewords in the dual codes [5]. Non-perfect secret sharing schemes were proposed [7] where the subsets of participants unable to reconstruct the secret could get some information about the secret. The term "tamp" is used in this scenario. It was shown in [8] that in secret sharing schemes based on linear codes, the amount of information leakage of the secret when some participants are corrupted is completely determined by the RGHWs of the involved codes.

The concept of RGHWs of linear codes is an extension of generalized Hamming weights (GHW) of linear codes, but the studies of RGHWs can not be substituted by those of GHWs. The concept of GHWs of linear codes was first introduced by Wei [9] to study the linear codes over wire-tap channel of type II and was later used by Ozarow and Wyner [10] in cryptography to characterize the performance of linear codes when used over such a channel. The GHWs of linear codes have been used in many other applications [11, 12, 13, 14, 15], so the study of GHWs of linear codes has attracted much attention in the past two decades. Comparing with GHWs, the RGHWs are defined on a pair of linear codes (a linear codes and one of its subcodes); the RGHWs have only one more restriction which makes they are often larger than the corresponding GHWs; and they should have applications parallelly to those of GHWs which need to be found in the future.

---

*Key words and phrases.* Relative generalized Hamming weight, cyclic codes, character sums, Gauss sums.

The second author is supported by NSFC No.11471178 and the Tsinghua National Lab. for Information Science and Technology.

The concept of RGHWs was proposed by Luo et al. [16] in their study of communication over the wire-tap channel of type II. They proved the equivalence between RGHW and the corresponding relative dimension/length profile (RDLP), similarly as the relation between the dimension/length profile and the GHW demonstrated by Forney [17]. Bounds on RGHWs and constructions of good codes are studied in [18, 19, 20].

So far, only few classes of linear codes have been examined for their RGHW/RDLP. In [21], RGHWs of almost all 4-dimensional linear code respect to its subcodes are determined by using techniques in finite projective geometry. In [8], the authors estimated RGHWs of general linear codes by Feng-Rao approach [22] and in particular they checked their bounds for one-point Hermitian codes. In [23], RGHWs of  $q$ -ary Reed-Muller codes are studied, closed formula expressions for  $q$ -ary Reed-Muller codes in two variables were presented, and simple and low complexity algorithm to determine RGHWs of general  $q$ -ary Reed-Muller codes were given by extension of Heijnen and Pellikaan method [24].

In this paper, we consider a special class of cyclic codes and give two formulae for their RGHWs. Section 2 reviews the definition of RGHW and introduces the cyclic codes we investigate. The one-to-one correspondence between the subspaces of the cyclic code and the subspaces of the direct product of two big fields is established. Equipped with this correspondence, one inner product on the direct product space of two big fields is defined to transfer the RGHW problem to a counting problem on the dual space. Hence, we obtain our first formula of RGHWs. By employing exponential sums, the common method in computing the weight distributions of cyclic codes, we get the second formula of RGHWs. As applications of the two formulae, explicit examples are calculated, and explicit formulae are given.

## 2. RELATIVE GENERALIZED HAMMING WEIGHTS OF CYCLIC CODES

In this section, we give two formulae for RGHWs of cyclic codes of two nonzeros respect to one of its irreducible cyclic subcodes.

We first introduce some notations valid for the whole paper.

- Let  $\mathbb{F}_q$  be the finite field of  $q$  elements with characteristic  $p$ . Denote an extension field of  $\mathbb{F}_q$  by  $\mathbb{F}_Q$ , and the trace map from  $\mathbb{F}_Q$  to  $\mathbb{F}_q$  by  $T_q^Q$ . Precisely, for any  $a \in \mathbb{F}_Q = \mathbb{F}_{q^m}$ , the trace  $T_q^Q$  of  $a$  is  $T_q^Q(a) = a + a^q + \cdots + a^{q^{m-1}}$ .
- Let  $V \subset \mathbb{F}_q^N$  be a  $k$ -dimensional linear space over  $\mathbb{F}_q$ . We also call  $V$  an  $[N, k]$  linear code over  $\mathbb{F}_q$ . For any  $1 \leq j \leq k$ , denote by  $\begin{bmatrix} V \\ j \end{bmatrix}_q$  the set of all  $j$ -dimensional linear subspaces of  $V$ .
- For any  $D \in \begin{bmatrix} V \\ j \end{bmatrix}_q$ , define the support of  $D$  to be the set of locations at which all the vectors in  $D$  are zeros. Denote by  $\text{Supp}(D)$  the support of  $D$ . That is,

$$\text{Supp}(D) = \{i : 1 \leq i \leq N, v_i \neq 0 \text{ for some } v = (v_1, \dots, v_N) \in D\}.$$

**Definition 2.1.** Let  $C_1 \subset C_2 \subset \mathbb{F}_q^N$  be two  $\mathbb{F}_q$  linear codes of dimension  $k_1, k_2$ , respectively. For  $1 \leq j \leq k_2 - k_1$ , the  $j$ th RGHW of  $C_2$  respect to its subcode  $C_1$  is defined to be the minimum size of  $\text{Supp}(D)$  where  $D$  runs through all  $j$ -dimensional linear subspaces of  $C_2$

among which everyone has intersection  $\{0\}$  with  $C_1$ . Denote it by  $M_j(C_2, C_1)$ . That is,

$$M_j(C_2, C_1) = \min \left\{ |\text{Supp}(D)| : D \in \begin{bmatrix} C_2 \\ j \end{bmatrix}_q, D \cap C_1 = \{0\} \right\}.$$

Note that if the restriction  $D \cap C_1 = \{0\}$  is released in the definition of RGHWs, then it becomes the corresponding GHW  $d_j$  of the code  $C_2$ .

Now we introduce the cyclic codes considered in this paper. Let  $\mathbb{F}_Q$  be a finite field with  $Q = q^m$ . Suppose  $\alpha_1, \alpha_2$  are two elements in  $\mathbb{F}_Q^*$  which are not conjugate to each other over  $\mathbb{F}_q$ . Let  $n_1, n_2$  be the orders of  $\alpha_1$  and  $\alpha_2$ , respectively. Let  $d = \gcd(n_1, n_2)$  and  $n = \frac{n_1 n_2}{d}$ . Suppose  $\gamma_1$  and  $\gamma_2$  are primitive elements of the fields  $\mathbb{F}_q(\alpha_1) = \mathbb{F}_{Q_1} = \mathbb{F}_{q^{k_1}}$  and  $\mathbb{F}_q(\alpha_2) = \mathbb{F}_{Q_2} = \mathbb{F}_{q^{k_2}}$ , respectively, then  $\alpha_i = \gamma_i^{e_i}$  and  $Q_i - 1 = e_i n_i$  for  $i = 1, 2$ .

With the above setting, we have two irreducible cyclic codes

$$C_i = \{c(\beta_i) = (T_q^{Q_i}(\beta_i), T_q^{Q_i}(\beta_i \alpha_i), \dots, T_q^{Q_i}(\beta_i \alpha_i^{n_i-1})) : \beta_i \in \mathbb{F}_{Q_i}\}$$

for  $i = 1, 2$ . It is easy to see that  $C_i$  has parameters  $[n_i, k_i]$ , and by Delsarte's theorem [25], the parity check polynomial  $h_i(x) \in \mathbb{F}_q[x]$  of  $C_i$  is the minimal (also irreducible) polynomial of  $\alpha_i^{-1}$  over  $\mathbb{F}_q$ , for  $i = 1, 2$ . The Hamming weight distributions of irreducible cyclic codes and general cyclic codes are studied extensively in the literature. Recently, the GHWs of irreducible cyclic codes are studied by the second author of this paper [1] and the GHWs of more special cyclic codes are presented in [26]. Using the method in [1], we compute the RGHWs of the following two cyclic codes:

$$(2.1) \quad C = \{c(\beta_1, \beta_2) : \beta_1 \in \mathbb{F}_{Q_1}, \beta_2 \in \mathbb{F}_{Q_2}\},$$

where

$$c(\beta_1, \beta_2) = (T_q^{Q_1}(\beta_1) + T_q^{Q_2}(\beta_2), T_q^{Q_1}(\beta_1 \alpha_1) + T_q^{Q_2}(\beta_2 \alpha_2), \dots, T_q^{Q_1}(\beta_1 \alpha_1^{n-1}) + T_q^{Q_2}(\beta_2 \alpha_2^{n-1})),$$

and its subcode

$$(2.2) \quad C' = \{c(0, \beta_2) : \beta_2 \in \mathbb{F}_{Q_2}\}.$$

Note that the codes  $C$  and  $C'$  have parameters  $[n, k_1 + k_2]$  and  $[n, k_2]$ , respectively, and the codeword  $c(0, \beta_2) \in C'$  is the repetition of the codeword  $c(\beta_2) \in C_2$  by  $\frac{n}{n_2}$  times. Again by Delsarte's theorem, the cyclic code  $C$  has parity check polynomial  $h_1(x)h_2(x)$ . Such a cyclic code  $C$  is often called cyclic code with two nonzeros, since the parity check polynomial factors through two distinct irreducible polynomials.

**2.1. The First Formula.** We first characterize the condition that subspaces of  $C$  have zero-intersection with  $C'$ , then give our first formula for  $M_j(C, C')$ .

From the definition of the cyclic code  $C$ , we have a canonical isomorphism of  $\mathbb{F}_q$ -linear spaces:

$$\mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \rightarrow C, \quad (\beta_1, \beta_2) \mapsto c(\beta_1, \beta_2).$$

So we get a one-one correspondence

$$(2.3) \quad \varphi : \begin{bmatrix} C \\ j \end{bmatrix}_q \rightarrow \begin{bmatrix} \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \\ j \end{bmatrix}_q.$$

For any  $D \in \begin{bmatrix} C \\ j \end{bmatrix}_q$ , under this correspondence, we have

$$D \cap C' = \{0\} \Leftrightarrow \varphi(D) \cap (\{0\} \times \mathbb{F}_{Q_2}) = \{0\}.$$

If we denote by  $\pi_i$  the projection of  $H = \varphi(D)$  at the  $i$ th coordinate:

$$\begin{aligned} \pi_1 : H &\rightarrow \mathbb{F}_{Q_1}, & (\beta_1, \beta_2) &\mapsto \beta_1; \\ \pi_2 : H &\rightarrow \mathbb{F}_{Q_2}, & (\beta_1, \beta_2) &\mapsto \beta_2, \end{aligned}$$

then

$$H \cap (\{0\} \times \mathbb{F}_{Q_2}) = \{0\} \Leftrightarrow \ker(\pi_1) = \{0\} \Leftrightarrow \text{Im}(\pi_1) \in \begin{bmatrix} \mathbb{F}_{Q_1} \\ j \end{bmatrix}_q.$$

Furthermore, an inner product on  $\mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2}$  is introduced as follows. For any  $(x_1, y_1), (x_2, y_2) \in \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2}$ , the inner product between the two elements is defined to be

$$\langle (x_1, y_1), (x_2, y_2) \rangle = T_q^{Q_1}(x_1 x_2) + T_q^{Q_2}(y_1 y_2) \in \mathbb{F}_q.$$

With respect to this inner product, the dual space of  $H$  is defined to be

$$H^\perp = \{v \in \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} : \langle v, w \rangle = 0, \forall w \in H\} \in \begin{bmatrix} \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \\ k_1 + k_2 - j \end{bmatrix}_q.$$

So the intersection property can be interpreted as following

$$H \cap (\{0\} \times \mathbb{F}_{Q_2}) = \{0\} \Leftrightarrow H^\perp + (\mathbb{F}_{Q_1} \times \{0\}) = \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \Leftrightarrow \pi_2(H^\perp) = \mathbb{F}_{Q_2}.$$

Now, with the preparation above, the first formula is presented in the following theorem.

**Theorem 2.1.** *Let  $C$  and  $C'$  be the cyclic codes given by (2.1) and (2.2), respectively. For  $1 \leq j \leq k_1$ , we have*

$$M_j(C, C') = n - N_j,$$

where

$$N_j = \max \left\{ |H \cap \langle (\alpha_1, \alpha_2) \rangle| : H \in \begin{bmatrix} \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \\ k_1 + k_2 - j \end{bmatrix}_q, \pi_2(H) = \mathbb{F}_{Q_2} \right\},$$

and  $\langle (\alpha_1, \alpha_2) \rangle$  denotes the subgroup  $\{(\alpha_1^i, \alpha_2^i) : 1 \leq i \leq n\}$  generated by  $(\alpha_1, \alpha_2)$ .

*Proof.* By definition, we have

$$\begin{aligned} M_j(C, C') &= \min \left\{ |\text{Supp}(D)| : D \in \begin{bmatrix} C \\ j \end{bmatrix}_q, D \cap C' = \{0\} \right\} \\ &= n - \max \left\{ N_j(D) : D \in \begin{bmatrix} C \\ j \end{bmatrix}_q, D \cap C' = \{0\} \right\}, \end{aligned}$$

where

$$\begin{aligned} N_j(D) &= |\{i : 0 \leq i \leq n-1, T_q^{Q_1}(\beta_1 \alpha_1^i) + T_q^{Q_2}(\beta_2 \alpha_2^i) = 0, \forall (\beta_1, \beta_2) \in D\}| \\ &= |\{i : 0 \leq i \leq n-1, \langle (\beta_1, \beta_2), (\alpha_1^i, \alpha_2^i) \rangle = 0, \forall (\beta_1, \beta_2) \in \varphi(D)\}| \\ &= |\{i : 0 \leq i \leq n-1, (\alpha_1^i, \alpha_2^i) \in \varphi(D)^\perp\}|. \end{aligned}$$

Together with the discussion previous of the theorem, one can easily obtain the theorem.  $\square$

**2.2. Applications of the First Formula.** As one application, taking  $q = 2$ ,  $Q_1 = 2^{k_1}$ ,  $Q_2 = 2^{k_2}$ ,  $e_1 = e_2 = 1$  such that  $\gcd(k_1, k_2) = 1$ ,  $k_1, k_2 \geq 2$ ,  $\alpha_i = \gamma_i$  is the primitive element of  $\mathbb{F}_{Q_i}$  for  $i = 1, 2$ . In this case,  $C_1, C_2$  are cyclic codes from  $m$ -sequences of degree  $k_1, k_2$ , respectively. Since  $\gcd(k_1, k_2) = 1$ , it follows that  $\gcd(n_1, n_2) = \gcd(Q_1 - 1, Q_2 - 1) = 1$ . So the length  $n = n_1 n_2$  and the group generated by  $(\alpha_1, \alpha_2)$

$$\langle (\alpha_1, \alpha_2) \rangle = \langle \alpha_1 \rangle \times \langle \alpha_2 \rangle = \mathbb{F}_{Q_1}^* \times \mathbb{F}_{Q_2}^*.$$

Hence, for any  $H \in \left[ \begin{smallmatrix} \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \\ k_1 + k_2 - j \end{smallmatrix} \right]_q$  ( $1 \leq j \leq k_1$ ), we have

$$\begin{aligned} & |H \cap \langle (\alpha_1, \alpha_2) \rangle| \\ &= |H \cap (\mathbb{F}_{Q_1}^* \times \mathbb{F}_{Q_2}^*)| \\ &= |\{(\beta_1, \beta_2) \in H : \beta_1 \beta_2 \neq 0\}| \\ &= q^{k_1 + k_2 - j} - |\pi_1^{-1}(0)| - |\pi_2^{-1}(0)| + 1. \end{aligned}$$

Taking account of the property  $\pi_2(H) = \mathbb{F}_{Q_2}$ ,  $\pi_2^{-1}(0)$  is an  $\mathbb{F}_q$ -linear subspace of  $H$  which has dimension

$$(k_1 + k_2 - j) - k_2 = k_1 - j$$

from the exact sequence of  $\mathbb{F}_q$ -linear spaces

$$\{0\} \rightarrow \pi_2^{-1}(0) \rightarrow H \rightarrow \pi_2(H) \rightarrow \{0\}.$$

So

$$|H \cap \langle (\alpha_1, \alpha_2) \rangle| = q^{k_1 + k_2 - j} - q^{k_1 - j} - |\pi_1^{-1}(0)| + 1.$$

By the same reason,  $\dim_{\mathbb{F}_q}(\pi_1^{-1}(0)) = k_1 + k_2 - j - \dim_{\mathbb{F}_q}(\pi_1(H)) \geq k_2 - j$ . On the other hand,  $\dim_{\mathbb{F}_q}(\pi_1^{-1}(0)) \leq \dim_{\mathbb{F}_q}(\{0\} \times \mathbb{F}_{Q_2}) = k_2$ . So,

$$k_2 - j \leq \dim_{\mathbb{F}_q}(\pi_1^{-1}(0)) \leq k_2,$$

and hence

$$q^{k_1 + k_2 - j} - q^{k_1 - j} - q^{k_2} + 1 \leq |H \cap \langle (\alpha_1, \alpha_2) \rangle| \leq q^{k_1 + k_2 - j} - q^{k_1 - j} - q^{k_2 - j} + 1.$$

Let  $H_1$  be the linear space spanning of  $v_i = (\alpha_1^i, \alpha_2^i)$ ,  $0 \leq i \leq k_1 - 1$ , over  $\mathbb{F}_q$ . Since  $\alpha_1^i$ ,  $0 \leq i \leq k_1 - 1$ , are linearly independent over  $\mathbb{F}_q$ , we have

$$\dim_{\mathbb{F}_q}(H_1) = k_1 - 1.$$

It is easy to see that the projection  $\pi_1 : H_1 \rightarrow \mathbb{F}_{Q_1}$  has kernel  $\ker(\pi_1) = \{0\}$ .

When  $k_2 \geq k_1$ , the projection  $\pi_2(H_1)$  is  $k_1$ -dimensional  $\mathbb{F}_q$ -linear subspace of  $\mathbb{F}_{Q_2}$  generated by  $\alpha_2^i$ ,  $0 \leq i \leq k_1 - 1$ . For  $1 \leq j \leq k_1$ ,  $m = k_1 + k_2 - j \geq k_2$ , so there is some  $(m - k_1)$ -dimensional  $\mathbb{F}_q$ -linear subspace  $V$  of  $\mathbb{F}_{Q_2}$  such that

$$V + \pi_2(H_1) = \mathbb{F}_{Q_2}.$$

Consider the subspace  $H = H_1 + (0, V)$  of  $\mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2}$ . It follows from  $\ker(\pi_1) = \{0\}$  that

$$H_1 \cap (0, V) = 0,$$

so the sum in  $H$  is a direct sum. Then

$$\dim_{\mathbb{F}_q}(H) = k_1 + (m - k_1) = m.$$

That is,  $H \in \left[ \begin{smallmatrix} \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \\ k_1 + k_2 - j \end{smallmatrix} \right]_q$ ,  $\pi_2(H) = V + \pi_2(H_1) = \mathbb{F}_{Q_2}$ , and  $\dim_{\mathbb{F}_q}(\pi_1^{-1}(0))$  achieves the minimum  $m - k_1 = k_2 - j$ . So

$$N_j = q^{k_1+k_2-j} - q^{k_1-j} - q^{k_2-j} + 1.$$

When  $1 \leq j \leq k_2 < k_1$ , the same construction as above can show that  $N_j$  has the same formula

$$N_j = q^{k_1+k_2-j} - q^{k_1-j} - q^{k_2-j} + 1.$$

When  $k_2 < j \leq k_1$ , we have  $k_2 \leq m = k_1 + k_2 - j < k_1$ . Taking  $H$  to be the  $\mathbb{F}_q$ -linear space spanning by  $(\alpha_1^i, \alpha_2^i), 0 \leq i \leq m - 1$ , as  $m \leq k_1$ , we know  $\dim_{\mathbb{F}_q}(H) = m$ . From  $m \geq k_2$ , it follows that  $\pi_2(H) = \mathbb{F}_{Q_2}$ . In this case,  $\pi_1^{-1}(0) = \{0\}$  achieves the minimal dimension. So

$$N_j = q^{k_1+k_2-j} - q^{k_1-j}.$$

In conclusion, we have the following corollary:

**Corollary 2.1.** *Let  $\alpha_1, \alpha_2$  be the primitive elements of  $\mathbb{F}_{Q_1}$  and  $\mathbb{F}_{Q_2}$ , respectively, where  $Q_1 = 2^{k_1}, Q_2 = 2^{k_2}, \gcd(k_1, k_2) = 1$ . Let  $C, C'$  be the cyclic codes defined by (2.1) and (2.2), respectively. For  $1 \leq j \leq k_1$ , we have*

$$M_j(C, C') = (Q_1 - 1)(Q_2 - 1) - N_j,$$

where if  $k_1 \leq k_2$ , then

$$N_j = q^{k_1+k_2-j} - q^{k_1-j} - q^{k_2-j} + 1;$$

if  $k_2 < k_1$ , then

$$N_j = \begin{cases} q^{k_1+k_2-j} - q^{k_1-j} - q^{k_2-j} + 1, & \text{if } 1 \leq j \leq k_2; \\ q^{k_1+k_2-j} - q^{k_1-j}, & \text{if } k_2 < j \leq k_1. \end{cases}$$

**2.3. The Second Formula.** The study of exponential sums, no matter the estimations or the exact values, is one important topic in number theory. Exponential sums, as a tool, are widely used in coding theory, such as the proof of MacWilliams identity, computing the minimum distance and weight distributions of codes, especially those of cyclic codes, etc. In this subsection, the exponential sums are used to present a formula for the RGHWS of the cyclic codes we consider in this paper.

We first review the Gauss sums over finite fields. A character of the abelian group  $(G, +)$  is a group homomorphism from  $G$  to the multiplicative group of nonzero complex numbers  $\mathbb{C}^*$ . Additive/multiplicative characters of a finite field  $\mathbb{F}_q$  are characters of the field considered as the additive group  $(\mathbb{F}_q, +)$  or multiplicative group  $(\mathbb{F}_q^*, \cdot)$ , respectively. For any multiplicative character  $\chi$  of  $\mathbb{F}_q$  and any  $\beta \in \mathbb{F}_q$ , the Gauss sum of  $\chi$  and  $\beta$  is defined to be the sum

$$G_q(\chi; \beta) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \zeta_p^{T_p^q(\beta x)},$$

where  $\zeta_l = e^{2\pi\sqrt{-1}/l}$  is the primitive  $l$ th root of unity, for any positive integer  $l$ . We always denote

$$G_q(\chi) = G_q(\chi; 1).$$

In particular, we have the following relationship

$$(2.4) \quad G_q(\chi; \beta) = \bar{\chi}(\beta) G_q(\chi)$$

where  $\bar{\chi}$  is the conjugation of  $\chi$  defined by  $\bar{\chi}(x) = \overline{\chi(x)}$  for any  $x \in \mathbb{F}_q$ . Also note that

$$G_q(\chi; 0) = \sum_{x \in \mathbb{F}_q^*} \chi(x) = \begin{cases} q-1, & \chi = 1; \\ 0, & \text{otherwise.} \end{cases}$$

is the complete sum of the character  $\chi$ . In general, we have the following character sum over finite abelian groups which can be viewed as the duality property.

**Lemma 2.1.** *Let  $\theta$  be a primitive element of  $\mathbb{F}_q$ . Let  $\chi$  be the multiplicative character of  $\mathbb{F}_q$  defined by  $\chi(\theta) = \zeta_e$ . For  $\alpha = \theta^e$ , and any  $x \in \mathbb{F}_q^*$ , we have*

$$\sum_{\lambda=0}^{e-1} \chi^\lambda(x) = \begin{cases} e, & \text{if } x \in \langle \alpha \rangle; \\ 0, & \text{otherwise,} \end{cases}$$

where  $\langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{e-1}\}$  is the subgroup generated by  $\alpha$ .

From the proof of Theorem 2.1, in order to compute  $M_j(C, C')$ , it is enough to compute

$$N_j(D) = |\{i : 0 \leq i \leq n-1, T_q^{Q_1}(\beta_1 \alpha_1^i) + T_q^{Q_2}(\beta_2 \alpha_2^i) = 0, \forall (\beta_1, \beta_2) \in D\}|$$

then take the maximum of  $N_j(D)$  where  $D$  runs over  $\begin{bmatrix} C \\ j \end{bmatrix}_q$  with  $D \cap C' = \{0\}$ .

For  $1 \leq j \leq k_1$ , any  $D \in \begin{bmatrix} C \\ j \end{bmatrix}_q$  with  $D \cap C' = \{0\}$ , take a basis  $\{(\beta_1^{(\lambda)}, \beta_2^{(\lambda)}) : 1 \leq \lambda \leq j\}$  for  $H = \varphi(D)$  over  $\mathbb{F}_q$ . Then

$$\begin{aligned} N_j(D) &= |\{i : 0 \leq i \leq n-1, T_q^{Q_1}(\beta_1 \alpha_1^i) + T_q^{Q_2}(\beta_2 \alpha_2^i) = 0, \forall (\beta_1, \beta_2) \in H\}| \\ &= |\{i : 0 \leq i \leq n-1, T_q^{Q_1}(\beta_1^{(\lambda)} \alpha_1^i) + T_q^{Q_2}(\beta_2^{(\lambda)} \alpha_2^i) = 0, \forall 1 \leq \lambda \leq j\}| \\ &= \frac{1}{q^j} \sum_{i=0}^{n-1} \prod_{\lambda=1}^j \sum_{x_t \in \mathbb{F}_q} \zeta_p^{T_p^q(x_t(T_q^{Q_1}(\beta_1^{(\lambda)} \alpha_1^i) + T_q^{Q_2}(\beta_2^{(\lambda)} \alpha_2^i)))} \\ &= \frac{1}{q^j} \sum_{i=0}^{n-1} \sum_{x_1, \dots, x_j \in \mathbb{F}_q} \zeta_p^{T_p^{Q_1}(\alpha_1^i(x_1 \beta_1^{(1)} + \dots + x_j \beta_1^{(j)})) + T_p^{Q_2}(\alpha_2^i(x_1 \beta_2^{(1)} + \dots + x_j \beta_2^{(j)}))} \\ &= \frac{1}{q^j} \sum_{i=0}^{n-1} \sum_{(\beta_1, \beta_2) \in H} \zeta_p^{T_p^{Q_1}(\beta_1 \alpha_1^i) + T_p^{Q_2}(\beta_2 \alpha_2^i)} \\ &= \frac{n}{q^j} + \frac{1}{q^j} (A + B), \end{aligned}$$

where

$$\begin{aligned}
A &= \sum_{i=0}^{n-1} \sum_{(\beta_1, 0) \in H, \beta_1 \neq 0} \zeta_p^{T_p^{Q_1}(\beta_1 \alpha_1^i)} \\
&= \frac{n}{n_1} \sum_{(\beta_1, 0) \in H, \beta_1 \neq 0} \sum_{x \in \langle \alpha_1 \rangle} \zeta_p^{T_p^{Q_1}(\beta_1 x)} \\
&\stackrel{(1)}{=} \frac{n}{e_1 n_1} \sum_{(\beta_1, 0) \in H, \beta_1 \neq 0} \sum_{x \in \mathbb{F}_{Q_1}^*} \zeta_p^{T_p^{Q_1}(\beta_1 x)} \sum_{\lambda=0}^{e_1-1} \chi^\lambda(x) \\
&\stackrel{(2)}{=} \frac{n}{e_1 n_1} \sum_{(\beta_1, 0) \in H, \beta_1 \neq 0} \sum_{\lambda=0}^{e_1-1} \bar{\chi}^\lambda(\beta_1) G_{Q_1}(\chi^\lambda) \\
&\stackrel{(3)}{=} \frac{n}{e_1 n_1} \sum_{\lambda=0, \chi^\lambda(\mathbb{F}_q^*)=1}^{e_1-1} G_{Q_1}(\chi^\lambda) \sum_{(\beta_1, 0) \in H, \beta_1 \neq 0} \bar{\chi}^\lambda(\beta_1),
\end{aligned}$$

where  $\chi$  is the multiplicative character of  $\mathbb{F}_{Q_1}$  such that  $\chi(\gamma) = \zeta_{e_1}$ ; and

$$B = \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} \sum_{i=0}^{n-1} \zeta_p^{T_p^{Q_1}(\beta_1 \alpha_1^i) + T_p^{Q_2}(\beta_2 \alpha_2^i)}.$$

The equality (1) follows from the relationship (2.4). The equality (2) follows from Lemma 2.1. The equality (3) follows from the property <sup>1</sup>: if  $\psi$  is a multiplicative character of  $\mathbb{F}_Q$  which is non-trivial over the subfield  $\mathbb{F}_q$ , and  $H$  is an  $\mathbb{F}_q$ -linear subspace of  $\mathbb{F}_Q$ , then the incomplete sum  $\sum_{x \in H} \psi(x) = 0$ .

So by using the above expression of  $N_j(D)$ , we give another formula for the RGHW  $M_j(C, C')$ .

### Discussion of $A$ and $B$ .

We now return to the property  $\chi^\lambda(\mathbb{F}_q^*) = 1$  ( $0 \leq \lambda \leq e_1 - 1$ ). Since  $\gamma_1^{\frac{Q_1-1}{q-1}}$  is a primitive element of  $\mathbb{F}_q$ , the property  $\chi^\lambda(\mathbb{F}_q^*) = 1$  is equivalent to

$$1 = \chi^\lambda(\gamma_1^{\frac{Q_1-1}{q-1}}) = \zeta_{e_1}^{\lambda \frac{Q_1-1}{q-1}},$$

which is also equivalent to

$$e_1 \mid \lambda \frac{Q_1-1}{q-1}, \text{ i.e., } \frac{e_1}{e'_1} \mid \lambda, \text{ where } e'_1 = \gcd(e_1, \frac{Q_1-1}{q-1}).$$

---

<sup>1</sup>The proof is very easy. Take any  $\theta \in \mathbb{F}_q$  such that  $\psi(\theta) \neq 1$ , then

$$\psi(\theta) \sum_{x \in H} \psi(x) = \sum_{x \in H} \psi(\theta x) = \sum_{x \in \theta H} \psi(x) = \sum_{x \in H} \psi(x)$$

which implies  $\sum_{x \in H} \psi(x) = 0$ .



So  $\lambda$  has the form  $\lambda = \frac{e_1}{e'_1}\tau$ ,  $0 \leq \tau \leq e'_1 - 1$ . Denote  $\psi = \chi^{e_1/e'_1}$ , then  $\psi(\gamma_1) = \zeta_{e'_1}$  and

$$\begin{aligned} A &= \frac{n}{e_1 n_1} \sum_{\lambda=0, \chi^\lambda(\mathbb{F}_q^*)=1}^{e_1-1} G_{Q_1}(\chi^\lambda) \sum_{(\beta_1, 0) \in H, \beta_1 \neq 0} \bar{\chi}^\lambda(\beta_1) \\ &= \frac{n}{e_1 n_1} \sum_{\tau=0}^{e'_1-1} G_{Q_1}(\psi^\tau) \sum_{(\beta_1, 0) \in H, \beta_1 \neq 0} \bar{\psi}^\tau(\beta_1) \\ &= -\frac{n|(\mathbb{F}_{Q_1}^*, 0) \cap H|}{e_1 n_1} + \frac{n}{e_1 n_1} \sum_{\tau=1}^{e'_1-1} G_{Q_1}(\psi^\tau) \sum_{(\beta_1, 0) \in H, \beta_1 \neq 0} \bar{\psi}^\tau(\beta_1). \end{aligned}$$

In particular, if  $e'_1 = 1$ , then

$$A = -\frac{n|(\mathbb{F}_{Q_1}^*, 0) \cap H|}{Q_1 - 1}.$$

We now study the exponential sum  $B$  provided that  $\gcd(n_1, n_2) = 1$ . In this case, the length  $n$  of the code  $C$  equals  $n_1 n_2$ . For any  $0 \leq i \leq n - 1$ , there is a unique pair  $(i_1, i_2)$  such that  $0 \leq i_1 \leq n_1 - 1$ ,  $0 \leq i_2 \leq n_2 - 1$  and

$$i = i_1 n_1 + i_2 n_2 \pmod{n}.$$

We can compute

$$\begin{aligned} B &= \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} \sum_{i=0}^{n-1} \zeta_p^{T_p^{Q_1}(\beta_1 \alpha_1^i) + T_p^{Q_2}(\beta_2 \alpha_2^i)} \\ &= \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} \left( \sum_{i_1=0}^{n_1-1} \zeta_p^{T_p^{Q_1}(\beta_1 \alpha_1^{n_2 i_1})} \right) \left( \sum_{i_2=0}^{n_2-1} \zeta_p^{T_p^{Q_2}(\beta_2 \alpha_2^{n_1 i_2})} \right) \\ &= \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} \left( \sum_{x_1 \in \langle \alpha_1 \rangle} \zeta_p^{T_p^{Q_1}(\beta_1 x_1)} \right) \left( \sum_{x_2 \in \langle \alpha_2 \rangle} \zeta_p^{T_p^{Q_2}(\beta_2 x_2)} \right) \\ &= \frac{1}{e_1 e_2} \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} \sum_{\lambda_1=0}^{e_1-1} \sum_{\lambda_2=0}^{e_2-1} G_{Q_1}(\chi_1^{\lambda_1}) G_{Q_2}(\chi_2^{\lambda_2}) \bar{\chi}_1^{\lambda_1}(\beta_1) \bar{\chi}_2^{\lambda_2}(\beta_2) \\ &= \frac{1}{e_1 e_2} \sum_{\substack{0 \leq \lambda_1 \leq e_1-1, \\ 0 \leq \lambda_2 \leq e_2-1, \\ \chi_1^{\lambda_1} \chi_2^{\lambda_2}(\mathbb{F}_q^*)=1}} G_{Q_1}(\chi_1^{\lambda_1}) G_{Q_2}(\chi_2^{\lambda_2}) \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} \bar{\chi}_1^{\lambda_1}(\beta_1) \bar{\chi}_2^{\lambda_2}(\beta_2) \end{aligned}$$

where  $\chi_i$  are the characters of  $\mathbb{F}_{Q_i}^*$  such that  $\chi_i(\gamma_i) = \zeta_{e_i}$ , for  $i = 1, 2$ . The condition  $\chi_1^{\lambda_1} \chi_2^{\lambda_2}(\mathbb{F}_q^*) = 1$  is equivalent to

$$\chi_1^{\lambda_1} \chi_2^{\lambda_2}(\delta) = 1$$

where  $\delta = \gamma_1^{\frac{Q_1-1}{q-1}} = \gamma_2^{\frac{Q_2-1}{q-1}}$  is a primitive element <sup>2</sup> of  $\mathbb{F}_q$ . So it is equivalent to

$$1 = \chi_1^{\lambda_1}(\gamma_1^{\frac{Q_1-1}{q-1}}) \chi_2^{\lambda_2}(\gamma_2^{\frac{Q_2-1}{q-1}}) = \zeta_{e_1}^{\lambda_1 \frac{Q_1-1}{q-1}} \zeta_{e_2}^{\lambda_2 \frac{Q_2-1}{q-1}}$$

which is also equivalent to

$$\lambda_1 e_2 \frac{Q_1-1}{q-1} + \lambda_2 e_1 \frac{Q_2-1}{q-1} \equiv 0 \pmod{e_1 e_2}.$$

**2.4. Application of the Second Formula.** Take  $e_1 = 1$ ,  $e_2 = q-1$ ,  $Q_1 = q^{k_1}$ ,  $Q_2 = q^{k_2}$  such that  $\gcd(k_1, k_2) = 1$  and  $2 \nmid k_2$ , then  $e'_1 = \gcd(e_1, \frac{Q_1-1}{q-1}) = 1$ ,  $n_1 = q^{k_1} - 1$ ,  $n_2 = \frac{Q_2-1}{q-1}$ , and  $\gcd(n_1, n_2) = 1$ . From  $e'_1 = 1$ , we know that

$$A = -\frac{n|(\mathbb{F}_{Q_1}^*, 0) \cap H|}{Q_1-1} = -\frac{(q^{k_2}-1)|(\mathbb{F}_{Q_1}^*, 0) \cap H|}{q-1}.$$

Next, we determine the exact value of  $B$ :

$$\begin{aligned} B &= \frac{1}{e_1 e_2} \sum_{\substack{0 \leq \lambda_1 \leq e_1-1, \\ 0 \leq \lambda_2 \leq e_2-1, \\ \chi_1^{\lambda_1} \chi_2^{\lambda_2}(\mathbb{F}_q^*)=1}} G_{Q_1}(\chi_1^{\lambda_1}) G_{Q_2}(\chi_2^{\lambda_2}) \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} \bar{\chi}_1^{\lambda_1}(\beta_1) \bar{\chi}_2^{\lambda_2}(\beta_2) \\ &= \frac{-1}{q-1} \sum_{\substack{0 \leq \lambda_2 \leq q-2, \\ \chi_2^{\lambda_2}(\mathbb{F}_q^*)=1}} G_{Q_2}(\chi_2^{\lambda_2}) \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} \bar{\chi}_2^{\lambda_2}(\beta_2). \end{aligned}$$

The condition  $\chi_2^{\lambda_2}(\mathbb{F}_q^*) = 1$  has been discussed twice before. One can use the same argument to derive that it is equivalent to

$$q-1 \mid \lambda_2 \frac{Q_2-1}{q-1}$$

By the assumption  $2 \nmid k_2$ , we have  $\gcd(q-1, \frac{Q_2-1}{q-1}) = 1$ . So  $\chi_2^{\lambda_2}(\mathbb{F}_q^*) = 1$  is equivalent to  $q-1 \mid \lambda_2$ . But  $0 \leq \lambda_2 \leq q-2$ , so the condition  $\chi_2^{\lambda_2}(\mathbb{F}_q^*) = 1$  holds if and only if  $\lambda_2 = 0$ . Hence, we get

$$B = \frac{1}{q-1} \sum_{(\beta_1, \beta_2) \in H, \beta_1 \beta_2 \neq 0} 1 = \frac{|(\mathbb{F}_{Q_1}^* \times \mathbb{F}_{Q_2}^*) \cap H|}{q-1}.$$

---

<sup>2</sup>In general,  $\gamma_1^{\frac{Q_1-1}{q-1}}$  and  $\gamma_2^{\frac{Q_2-1}{q-1}}$  may differ from some element of  $\mathbb{F}_q$ . But this is not essential. By choosing carefully  $\gamma_1$  and  $\gamma_2$  at the beginning, we can ensure  $\gamma_1^{\frac{Q_1-1}{q-1}} = \gamma_2^{\frac{Q_2-1}{q-1}}$ .

In conclusion, for any  $1 \leq j \leq k_1$ , any  $D \in \begin{bmatrix} C \\ j \end{bmatrix}_q$  with  $D \cap C' = \{0\}$ , let  $H = \varphi(D) \in \begin{bmatrix} \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \\ j \end{bmatrix}_q$ , then  $(0, \mathbb{F}_{Q_2}) \cap H = \{(0, 0)\}$  and

$$\begin{aligned} N_j(D) &= \frac{n}{q^j} + \frac{1}{q^j}(A + B) \\ &= \frac{n}{q^j} + \frac{1}{q^j} \left( -\frac{(q^{k_2} - 1)|(\mathbb{F}_{Q_1}^*, 0) \cap H|}{q - 1} + \frac{|(\mathbb{F}_{Q_1}^* \times \mathbb{F}_{Q_2}^*) \cap H|}{q - 1} \right) \\ &= \frac{n}{q^j} + \frac{1}{q^j} \left( -\frac{q^{k_2}|(\mathbb{F}_{Q_1}^*, 0) \cap H|}{q - 1} + \frac{|(\mathbb{F}_{Q_1}^* \times \mathbb{F}_{Q_2}^*) \cap H|}{q - 1} \right) \\ &= \frac{n}{q^j} + \frac{1}{q^j} \left( -\frac{q^{k_2}|(\mathbb{F}_{Q_1}, 0) \cap H|}{q - 1} + \frac{|(\mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2}) \cap H|}{q - 1} + \frac{q^{k_2} - 1}{q - 1} \right) \\ &= \frac{q^{k_1+k_2} - q^{k_1} + q^j - q^{k_2}|(\mathbb{F}_{Q_1}, 0) \cap H|}{q^j(q - 1)}. \end{aligned}$$

So in order to make  $N_j(D)$  large, we need to find  $H \in \begin{bmatrix} \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \\ j \end{bmatrix}_q$  such that  $(0, \mathbb{F}_{Q_2}) \cap H = \{(0, 0)\}$ , and  $|(\mathbb{F}_{Q_1}, 0) \cap H|$  is small.

When  $k_1 \leq k_2$ , take  $H$  as the  $\mathbb{F}_q$ -spanning space of  $\{(v_1, e_1), \dots, (v_j, e_j)\}$  where  $v_1, \dots, v_j$  form a partial basis of  $\mathbb{F}_{Q_1}$  and  $e_1, \dots, e_j$  form a partial basis of  $\mathbb{F}_{Q_2}$ . Then  $H \in \begin{bmatrix} \mathbb{F}_{Q_1} \times \mathbb{F}_{Q_2} \\ j \end{bmatrix}_q$  satisfies  $(0, \mathbb{F}_{Q_2}) \cap H = \{(0, 0)\}$  and

$$|(\mathbb{F}_{Q_1}, 0) \cap H| = 1$$

achieves the minimum. So in this case, we have

$$M_j(C, C') = n - \frac{q^{k_1+k_2} - q^{k_1} + q^j - q^{k_2}}{q^j(q - 1)} = n + \sum_{\iota=0}^{k_1-j-1} q^\iota - \sum_{\kappa=k_2-j}^{k_1+k_2-j-1} q^\kappa.$$

When  $j \leq k_2 < k_1$ , take the same space  $H$  as above, then we obtain the same result

$$M_j(C, C') = n - \frac{q^{k_1+k_2} - q^{k_1} + q^j - q^{k_2}}{q^j(q - 1)} = n + \sum_{\iota=0}^{k_2-j-1} q^\iota - \sum_{\kappa=k_1-j}^{k_1+k_2-j-1} q^\kappa.$$

When  $k_2 < j \leq k_1$ , the canonical isomorphisms of  $\mathbb{F}_q$ -linear spaces

$$\frac{H}{(\mathbb{F}_{Q_1}, 0) \cap H} \cong \frac{(\mathbb{F}_{Q_1}, 0) + H}{(\mathbb{F}_{Q_1}, 0)} \cong \pi_2(H)$$

induce  $j - \dim_{\mathbb{F}_q}((\mathbb{F}_{Q_1}, 0) \cap H) = \dim_{\mathbb{F}_q}(\pi_2(H)) \leq k_2$ . So

$$\dim_{\mathbb{F}_q}((\mathbb{F}_{Q_1}, 0) \cap H) \geq j - k_2.$$

On the other hand, we will show the equality is available for some  $H$ . Let  $m = k_1 + k_2 - j$ , then  $k_2 \leq m < k_1$ . Taking  $H$  to be the  $\mathbb{F}_q$ -linear space spanning by  $(\alpha_1^i, \alpha_2^i), 0 \leq i \leq m - 1$ ,

as  $m \leq k_1$ , we know  $\dim_{\mathbb{F}_q}(H) = m$  and  $(0, \mathbb{F}_{Q_2}) \cap H = \{(0, 0)\}$ . In this case,  $(\mathbb{F}_{Q_1}, 0) \cap H$  achieves the minimal dimension  $j - k_2$ . So

$$M_j(C, C') = n - \frac{q^{k_1+k_2} - q^{k_1} + q^j - q^{k_2}q^{j-k_2}}{q^j(q-1)} = n - q^{k_1-j} \sum_{\iota=0}^{k_2-1} q^\iota.$$

From the discussion above, we have the following corollary as an application of our second formula:

**Corollary 2.2.** *Let  $\gamma_1$  and  $\gamma_2$  be two primitive elements of  $\mathbb{F}_{Q_1}$  and  $\mathbb{F}_{Q_2}$ , respectively, where  $Q_1 = q^{k_1}, Q_2 = q^{k_2}, \gcd(k_1, k_2) = 1$  and  $2 \nmid k_2$ . Take  $e_1 = 1, e_2 = q - 1$  and  $\alpha_i = \gamma_i^{e_i}$  for  $i = 1, 2$ . Let  $n_i$  be the order of  $\alpha_i$ , for  $i = 1, 2$ . Let  $C, C'$  be the cyclic codes defined by (2.1) and (2.2), respectively. Then the length of  $C$  and  $C'$  is  $n = n_1 n_2 = (Q_1 - 1)(Q_2 - 1)/(q - 1)$ . For  $1 \leq j \leq k_1$ , the  $j$ th RGHW of  $C$  respect to  $C'$  is*

$$M_j(C, C') = n - N_j,$$

where if  $k_1 \leq k_2$ , then

$$N_j = \sum_{\kappa=k_2-j}^{k_1+k_2-j-1} q^\kappa - \sum_{\iota=0}^{k_1-j-1} q^\iota;$$

if  $k_2 < k_1$ , then

$$N_j = \begin{cases} \sum_{\kappa=k_1-j}^{k_1+k_2-j-1} q^\kappa - \sum_{\iota=0}^{k_2-j-1} q^\iota, & \text{if } 1 \leq j \leq k_2; \\ q^{k_1-j} \sum_{\iota=0}^{k_2-1} q^\iota, & \text{if } k_2 < j \leq k_1. \end{cases}$$

Similarly, one can show

**Corollary 2.3.** *Let  $\gamma_1$  and  $\gamma_2$  be two primitive elements of  $\mathbb{F}_{Q_1}$  and  $\mathbb{F}_{Q_2}$ , respectively, where  $Q_1 = q^{k_1}, Q_2 = q^{k_2}, \gcd(k_1, k_2) = 1$  and  $2 \nmid k_1$ . Take  $e_1 = q - 1, e_2 = 1$  and  $\alpha_i = \gamma_i^{e_i}$  for  $i = 1, 2$ . Let  $n_i$  be the order of  $\alpha_i$ , for  $i = 1, 2$ . Let  $C, C'$  be the cyclic codes defined by (2.1) and (2.2), respectively. Then the length of  $C$  and  $C'$  is  $n = n_1 n_2 = (Q_1 - 1)(Q_2 - 1)/(q - 1)$ . For  $1 \leq j \leq k_1$ , the  $j$ th RGHW of  $C$  respect to  $C'$  is*

$$M_j(C, C') = n - N_j,$$

where if  $k_1 \leq k_2$ , then

$$N_j = \sum_{\kappa=k_2-j}^{k_1+k_2-j-1} q^\kappa - \sum_{\iota=0}^{k_1-j-1} q^\iota;$$

if  $k_2 < k_1$ , then

$$N_j = \begin{cases} \sum_{\kappa=k_1-j}^{k_1+k_2-j-1} q^\kappa - \sum_{\iota=0}^{k_2-j-1} q^\iota, & \text{if } 1 \leq j \leq k_2; \\ q^{k_1-j} \sum_{\iota=0}^{k_2-1} q^\iota, & \text{if } k_2 < j \leq k_1. \end{cases}$$

### 3. CONCLUSIONS

In this paper, we give two general formulae for the RGHWs of the cyclic codes with two nonzeros respect to one of its two irreducible cyclic subcodes. By using the formulae, RGHWs of two explicit classes of cyclic codes are obtained. Comparing with the computation of GHWs of the linear code, RGHWs have one more restriction which is difficult to describe or satisfy in general when one applies the techniques from computing GHWs. For example,

if one wants to compute the RGHWs of irreducible cyclic codes by using the method in this paper, then the restriction on the intersection with the subcode is hard to describe. So the method in this paper is not suitable in this scenario. We leave this problem as a future research problem.

## REFERENCES

- [1] M. Yang, J. Li, K. Feng, and D. Lin, “Generalized Hamming weights of irreducible cyclic codes,” to appear in *IEEE Transactions on Information Theory* 2015. Available: <http://arxiv.org/abs/1410.2702>.
- [2] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, pp. 612–613, Nov. 1979.
- [3] R. J. McEliece and D. V. Sarwate, “On sharing secrets and Reed-Solomon codes,” *Commun. ACM*, vol. 24, pp. 583–584, Sept. 1981.
- [4] H. Chen and R. Cramer, “Algebraic geometric secret sharing schemes and secure multi-party computation over small fields,” in *Proceedings of 26th Annual IACR CRYPTO, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 4117*, pp. 516–531, 2006.
- [5] J. L. Massey, “Minimal codewords and secret sharing,” in *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pp. 276–279, 1993.
- [6] H. Chen, S. Ling, and C. Xing, “Access structures of elliptic secret sharing schemes,” *IEEE Transactions on Information Theory*, vol. 54, pp. 850–852, feb. 2008.
- [7] G. Blakley and C. Meadows, “Security of ramp schemes,” in *Advances in Cryptology* (G. Blakley and D. Chaum, eds.), vol. 196 of *Lecture Notes in Computer Science*, pp. 242–268, Springer Berlin Heidelberg, 1985.
- [8] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and Y. Luo, “Relative generalized Hamming weights of one-point algebraic geometric codes,” *IEEE Transactions on Information Theory*, vol. 60, pp. 5938–5949, Oct 2014.
- [9] V. Wei, “Generalized Hamming weights for linear codes,” *IEEE Transactions on Information Theory*, vol. 37, pp. 1412–1418, Sep 1991.
- [10] L. Ozarow and A. Wyner, “Wire-tap channel II,” in *Advances in Cryptology* (T. Beth, N. Cot, and I. Ingemarsson, eds.), vol. 209 of *Lecture Notes in Computer Science*, pp. 33–50, Springer Berlin Heidelberg, 1985.
- [11] V. Guruswami, “List decoding from erasures: bounds and code constructions,” *IEEE Transactions on Information Theory*, vol. 49, pp. 2826–2833, Nov 2003.
- [12] T. Helleseth and P. V. Kumar, “The weight hierarchy of the Kasami codes,” *Discrete Mathematics*, vol. 145, no. 1C3, pp. 133 – 143, 1995.
- [13] H. Janwa and A. Lal, “On generalized Hamming weights and the covering radius of linear codes,” in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (S. Bozta? and H.-F. Lu, eds.), vol. 4851 of *Lecture Notes in Computer Science*, pp. 347–356, Springer Berlin Heidelberg, 2007.
- [14] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, “On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes,” *IEEE Transactions on Information Theory*, vol. 39, pp. 242–245, Jan 1993.
- [15] C.-K. Ngai, R. Yeung, and Z. Zhang, “Network generalized Hamming weight,” *IEEE Transactions on Information Theory*, vol. 57, pp. 1136–1143, Feb 2011.
- [16] Y. Luo, C. Mitropant, A. Vinck, and K. Chen, “Some new characters on the wire-tap channel of type II,” *IEEE Transactions on Information Theory*, vol. 51, pp. 1222–1229, March 2005.
- [17] G. D. F. Jr., “Dimension/length profiles and trellis complexity of linear block codes,” *IEEE Transactions on Information Theory*, vol. 40, no. 6, pp. 1741–1752, 1994.
- [18] Z. Zhuang, Y. Luo, A. Vinck, and B. Dai, “Some new bounds on relative generalized Hamming weight,” in *2011 IEEE 13th International Conference on Communication Technology (ICCT)*, pp. 971–974, Sept 2011.
- [19] Z. Zhuang, Y. Luo, and B. Dai, “Code constructions and existence bounds for relative generalized Hamming weight,” *Designs, Codes and Cryptography*, vol. 69, no. 3, pp. 275–297, 2013.
- [20] O. Geil, S. Martin, U. Martínez-Peñas, R. Matsumoto, and D. Ruano, “Asymptotically good ramp secret sharing schemes,” *arXiv preprint arXiv:1502.05507*, 2015.

- [21] Z. Liu, W. Chen, and Y. Luo, “The relative generalized Hamming weight of linear  $q$ -ary codes and their subcodes,” *Designs, Codes and Cryptography*, vol. 48, no. 2, pp. 111–123, 2008.
- [22] G.-L. Feng and T. Rao, “Decoding algebraic-geometric codes up to the designed minimum distance,” *IEEE Transactions on Information Theory*, vol. 39, pp. 37–45, Jan 1993.
- [23] S. Martin and O. Geil, “Relative generalized Hamming weights of  $q$ -ary reed-muller codes,” *arXiv preprint arXiv:1407.6185*, 2014.
- [24] P. Heijnen and R. Pellikaan, “Generalized Hamming weights of  $q$ -ary Reed-Muller codes,” *IEEE Transactions on Information Theory*, vol. 44, pp. 181–196, Jan 1998.
- [25] P. Delsarte, “On subfield subcodes of modified Reed-Solomon codes (Corresp.),” *IEEE Transactions on Information Theory*, vol. 21, pp. 575–576, Sept. 1975.
- [26] M. Xiong, S. Li, and G. Ge, “The weight hierarchy of some reducible cyclic codes,” *arXiv preprint arXiv:1504.01274*, 2015.

SCHOOL OF MATHEMATICAL SCIENCES, CAPITAL NORMAL UNIVERSITY, BEIJING 100048, P.R. CHINA  
*E-mail address:* junz@cnu.edu.cn

DEPARTMENT OF MATHEMATICS, TSINGHUA UNIVERSITY, BEIJING 100084, P.R. CHINA  
*E-mail address:* kfeng@math.tsinghua.edu.cn